

**Management Advisory Report: Follow-on  
Review of Lost or Stolen Sensitive Items of  
Inventory at the Internal Revenue Service**

**March 2002**

**Reference Number: 2002-10-065**

**This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.**



DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

INSPECTOR GENERAL  
for TAX  
ADMINISTRATION

March 8, 2002

MEMORANDUM FOR COMMISSIONER ROSSOTTI

A handwritten signature in cursive script, reading "Pamela J. Gardiner".

FROM: Pamela J. Gardiner  
Deputy Inspector General for Audit

SUBJECT: Final Management Advisory Report - Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service (Audit # 200210015)

This report presents the results of our follow-on review of lost or stolen sensitive items of inventory. The overall objective of this limited scope review was to assess the sufficiency of Internal Revenue Service (IRS) systems and procedures in providing select management information concerning missing computers and other sensitive items of inventory, such as value of the loss, associated employee disciplinary actions, and possible disclosure of taxpayer data. We also assessed the sufficiency of controls used to protect taxpayer information that is stored on laptop computers. The scope of our review involved a sample of missing computers, and all identified other sensitive items of inventory as reported by the IRS and included in our previous report.<sup>1</sup> This review was conducted at the request of Senator Charles E. Grassley, Ranking Member of the Senate Committee on Finance.

In summary, and as described in our previous report, we found that the IRS' inventory controls, including documentation to fully support the disposition of missing items, is insufficient to adequately account for its inventory of computers, firearms, and other sensitive items of inventory. Specifically, we found that a majority of the missing items of inventory previously reported were the result of items that could not be accounted for during physical inventories; potential disciplinary actions associated with some missing items were not evident from the documentation that was provided by the IRS; a determination of taxpayer information stored on computers that were unaccountable

---

<sup>1</sup> *Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service* (Reference Number: 2002-10-030, dated November 2001).

during physical inventories could not be made; encryption of taxpayer information indicated vulnerabilities to unauthorized disclosure; and, required forms to report and control missing items were often not complete.

Management's Response: IRS management agreed with our recommendations and is taking appropriate corrective actions. The Chief Information Officer and Chiefs of Criminal Investigation and Agency-Wide Shared Services will jointly issue an alert re-emphasizing the requirement to completely prepare the appropriate form, when warranted. Actions are currently underway to encrypt sensitive but unclassified information on all laptop computers, without negatively affecting ongoing work being performed on older laptop computers. New laptop computers are being configured with software to encrypt taxpayer information. IRS employees have been instructed on the need to encrypt files containing taxpayer information. Action will be taken to reiterate this requirement where the encryption capability has not been used.

Management's response to the draft report is included as Appendix IV. Their response did not specifically identify the responsible officials, implementation dates, or corrective action monitoring plans; we will follow up with IRS management to obtain this information.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Daniel R. Devlin, Assistant Inspector General for Audit (Headquarters Operations and Exempt Organizations Programs), at (202) 622-8500.

Attachments (2)

**Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of  
Inventory at the Internal Revenue Service**

---

**Table of Contents**

|  |         |
|--|---------|
| Background .....   | Page 1  |
| Value of Missing Computers and Identification of Lost,<br>Stolen, or Destroyed Status.....                         | Page 3  |
| Value of Missing Investigative Items of Inventory and<br>Identification of Lost, Stolen, or Destroyed Status ..... | Page 3  |
| Disciplinary Actions Taken and Government Reimbursement.....   | Page 6  |
| Missing Computers Containing Confidential Taxpayer<br>Information.....   | Page 9  |
| Sufficiency of File Encryption Practices.....  | Page 9  |
| Reports of Survey (Forms 1933) Not Properly Filed.....   | Page 11 |
| <u>Recommendations 1 and 2:</u> .....  | Page 14 |
| Appendix I – Detailed Objectives, Scope, and Methodology .....   | Page 15 |
| Appendix II – Major Contributors to This Report.....   | Page 17 |
| Appendix III – Report Distribution List .....  | Page 18 |
| Appendix IV – Management’s Response to the Draft Report .....  | Page 19 |

## Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

---

---

### Background

---

This review was conducted at the request of Senator Charles E. Grassley, Ranking Member of the Senate Committee on Finance. Senator Grassley, in a letter dated January 9, 2002, expressed concerns over the results of our initial review of lost or stolen sensitive items of inventory at the Internal Revenue Service (IRS),<sup>1</sup> which was also performed at the Committee's request. In his request, Senator Grassley asked that we conduct follow-on work on a sample basis to obtain additional information concerning IRS-reported lost or stolen sensitive items of inventory.

In his request, Senator Grassley specifically asked that the Treasury Inspector General for Tax Administration (TIGTA) continue testing to obtain additional information concerning the following.

- Identify the approximate value at the time of the loss for a representative sample of the 2,332 missing computers. Also, identify whether the missing computers were lost, stolen, or destroyed.
- Identify the approximate value at the time of the loss for the 6 lost or stolen firearms, and the missing 50 communications devices, 40 identification badges, and 15 electronic surveillance devices. Also, identify whether the missing items were lost, stolen, or destroyed.
- Identify the types of disciplinary actions taken against employees or senior managers found to be responsible for the theft or loss of a computer. Specifically, identify what follow-up actions were taken, and if IRS employees including senior managers reimbursed the government for missing computers. Also, identify if any individual was involved with multiple missing computers.
- Determine for the sampled computers how many contained confidential taxpayer information.

---

<sup>1</sup> *Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service* (Reference Number: 2002-10-030, dated November 2001).

## Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

---

- Assess the sufficiency of IRS encryption practices to prevent the unauthorized disclosure of taxpayer information when a computer is lost or stolen.
- Provide copies of all documents, including completed Reports of Survey (Forms 1933), obtained in the follow-on review. Also, identify the responsible managers who failed to properly file a Form 1933.

Our review was conducted at the National Headquarters in Washington, DC, and the San Francisco and Atlanta posts-of-duty during the period December 2001 through February 2002. This work was performed mainly in the Offices of the Deputy Commissioner for Modernization and Chief Information Officer (CIO), and the Chief, Criminal Investigation (CI). Our limited encryption testing was performed in a Small Business/Self Employed Division group in the San Francisco post-of-duty and in a Tax Exempt and Government Entities Division group in the Atlanta post-of-duty. The review was conducted in accordance with the President's Council on Integrity and Efficiency's *Quality Standards for Inspections*. Detailed information on our review objectives, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

During the review, we coordinated our work with the Department of the Treasury Office of Inspector General and the General Accounting Office (GAO), both of whom are performing similar reviews of sensitive inventory items in other Treasury bureaus and government agencies, respectively.

We are presenting the results of our review by addressing each of the six elements separately. The information and data we obtained are what the IRS reported to us. We did not independently verify this data; accordingly, we express no opinion on the accuracy or completeness of the data. These results also further support the opinion, expressed in our first report, that the IRS continues to experience longstanding difficulties in maintaining reliable and accurate inventory information. The IRS has reported progress in addressing this weakness.

## **Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service**

---

---

### **Value of Missing Computers and Identification of Lost, Stolen, or Destroyed Status**

---

Based on documentation provided by the IRS, we were able to classify a representative sample of 100 missing computers as follows:

- 68 – Unaccountable during a physical inventory
- 13 – Disposed of without updating the inventory records
- 12 – Subsequently located by the IRS
- 2 – Lost in transit
- 1 – Stolen
- 4 – No documentation provided

For valuation purposes, we used an average 3-year useful life for the missing computers, the same used by the IRS for financial reporting. Using IRS-provided acquisition amounts, the 71 unaccountable, lost, and stolen computers had an initial acquisition cost of approximately \$212,500. Comparison of the acquisition dates and the reported loss dates showed that 59 of the 71 computers were acquired in excess of 3 years prior to the loss, and thus would be fully depreciated. Using a straight-line depreciation method, the depreciated value of the remaining 12 computers would be approximately \$11,500.

We are unable to comment on the four missing computers for which no documentation was provided. We also cannot determine whether the 68 computers unaccounted for during a physical inventory were lost, stolen, excessed, or otherwise disposed of. However, 57 of the 68 were older than 3 years. In addition, we did not independently verify the physical existence of the 12 computers that were subsequently located by the IRS.

---

### **Value of Missing Investigative Items of Inventory and Identification of Lost, Stolen, or Destroyed Status**

---

Of the six missing firearms, one was lost and five were stolen. Three of the stolen firearms were subsequently recovered. The cost of the lost firearm was reimbursed by private insurance. The initial acquisition cost of the remaining two stolen firearms was approximately \$1,200. Applying a useful life of 10 years for firearms, the total value of the 2 firearms would have been less than \$61 at the time of the loss considering their acquisition and loss dates.

## Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

---

Based on documentation provided by the IRS, we were able to classify the missing 50 communication devices, 40 identification badges/commissions, and 15 electronic surveillance devices as follows:<sup>2</sup>

### 50 - Communication Devices

- 35 – Unaccountable during a physical inventory
- 2 – Lost
- 2 – Subsequently located by the IRS
- 4 – Item lost in excess of 3 years ago
- 7 – Duplicate reporting<sup>3</sup>

In addition, during our more detailed review, we identified one additional communication device that was unaccountable during physical inventory. Adding this item to the total, and removing the 4 items lost in excess of 3 years ago, the 7 duplicate reporting items, and the 2 subsequently located items, brings the total of missing communication devices to 38 that were missing in the last 3 years.

The IRS provided completed Forms 1933, which identified acquisition amounts and dates for 29 of the 38 unaccountable and lost items. These forms showed an initial acquisition cost of approximately \$120,700 for these 29 items. For valuation purposes, we used an average 10-year useful life for the missing communication devices, which is the period used by the IRS for this type of

---

<sup>2</sup> In our initial review, we reported that the missing 50 communications devices and 15 electronic surveillance devices could compromise the public's safety or ongoing investigations. This was based on the general definitions of the respective inventory codes. Subsequent detailed analysis and discussions with CI staff during our second review indicated that the risk of compromising the public's safety or ongoing investigations, as initially reported, is diminished because of these items' functionality and age.

<sup>3</sup> Due to the CI reorganization and resulting change in jurisdictions of the management of CI field offices, the same record was contained in more than one office submission of documentation. We discovered these duplicate records only when scheduling the details of this documentation.



## **Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service**

---

equipment. Comparison of the acquisition dates and the reported loss dates showed that 12 of the 29 items were acquired in excess of 10 years prior to the loss. Assuming a straight-line depreciation method, the depreciated value of the remaining 17 items would be approximately \$29,700.

We were unable to accurately value 9 of the 38 items for which acquisition amounts and/or dates were not provided. All 9 items affected were unaccountable during a physical inventory. We also cannot determine whether the 36 items unaccounted for during a physical inventory were lost, stolen, excessed, or otherwise disposed of. In addition, we did not independently verify the physical existence of the two items that were subsequently located by the IRS.

### 40 - Identification Badges/Commissions

- 20 – Lost
- 13 – Stolen
- 4 – Item lost in excess of 3 years ago
- 3 – Duplicate reporting

CI identification badges and commissions have a nominal acquisition amount and an indefinite useful life. Therefore, a depreciated value of these items cannot be measured monetarily, and is not relevant. The real measurable impact of these missing items is how an unauthorized individual can use them. For example, one may attempt to impersonate an IRS Special Agent. However, we are not aware of any such attempts using the lost or stolen badges/commissions identified in this report.

### 15 - Electronic Surveillance Devices

- 14 – Unaccountable during a physical inventory
- 1 – Duplicate reporting

The IRS provided completed Forms 1933, which identified acquisition amounts and dates for 12 of the 14 unaccountable items. These forms showed an initial acquisition cost of approximately \$22,700. For valuation purposes, we used an average 10-year useful life for the missing electronic surveillance devices. Comparison of

## **Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service**

---

the acquisition dates and the reported loss dates showed that 4 of the 12 items were acquired in excess of 10 years prior to the loss. Assuming a straight-line depreciation method, the depreciated value of the remaining 8 items would be approximately \$7,800.

We were unable to accurately value 2 of the 14 items for which acquisition amounts and/or dates were not provided. Both items affected were unaccountable during physical inventory. We also cannot determine whether the 14 items unaccounted for during a physical inventory were lost, stolen, excessed, or otherwise disposed of.

---

### **Disciplinary Actions Taken and Government Reimbursement**

---

#### **Computers**

From the documentation that the IRS provided, we could not determine whether disciplinary action, including reimbursement, was taken against any employee or senior manager associated with the 68 computers that were unaccounted for during a physical inventory, or the 2 lost and 1 stolen computers. Further, we are unable to comment on the four missing computers for which the IRS did not provide any documentation concerning the missing condition.

The specific circumstances surrounding the 68 computers that were unaccounted for during a physical inventory are unknown, since the computers were reported in bulk and not individually reported as lost or stolen on separate Forms 1933. Therefore, we are unable to answer the questions concerning disciplinary actions taken or employee reimbursements received for these computers, other than to state that no disciplinary actions were evident from the documentation provided. An analysis of these computers showed that 57 of the 68 were in excess of 3 years old at the time of the loss; 37 of the 57 were in excess of 6 years old at the time of the loss.

The first of the two lost computers was misplaced during shipment from the manufacturer after repairs were completed. This computer was subsequently replaced by the manufacturer. The second lost computer was scheduled for excess and was misplaced during shipment to a Volunteer Income Tax Assistance program coordinator.

## **Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service**

---

Documentation provided by the IRS did not indicate whether any disciplinary action was taken. The IRS procured this computer in September 1995, and it was lost in December 2000.

The one stolen computer involved a situation where the computer was being transferred from one IRS building to another. Based on the documentation provided, the computer was removed from the building by someone other than the authorized movers. Documentation provided by the IRS did not indicate whether any disciplinary action was taken. This instance was referred to the TIGTA for investigation. The IRS procured this computer in May 1998, and it was stolen in August 2001.

### **Investigative Items**

As stated in our initial report, the IRS reported 1 lost and 5 stolen firearms for the past 3 years. Three of the stolen firearms were subsequently recovered. Disciplinary actions and reimbursements to the government for the six firearms were as follows:

- December 22, 1998 -- Vehicle broken into and firearm stolen that was later recovered. Employee reimbursed the government for the depreciated value of the firearm. Employee later reimbursed when firearm was recovered.
- March 17, 1999 -- Vehicle broken into and firearm stolen that was later recovered. Employee was required to reimburse the government until the firearm was subsequently recovered.
- April 26, 1999 -- Firearm involved in a boating accident. No disciplinary actions were deemed necessary. Cost of the firearm was reimbursed by the at-fault boater's insurance company.
- October 21, 1999 -- Vehicle entered into and firearm stolen that was later recovered. Employee was given a suspension.
- May 3, 2000 -- Vehicle broken into and firearm stolen. Employee reimbursed the government for

## **Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service**

---

the depreciated value of the firearm and was given a suspension.

- August 15, 2001 -- Vehicle broken into and firearm stolen. Although the documentation indicated that no disciplinary actions were deemed necessary at the time, CI staff advised that actions are pending.

As with the missing computers, the specific circumstances surrounding the 36 communication devices and 14 surveillance devices that were unaccounted for during a physical inventory are unknown, since the items were reported in bulk and not individually reported as missing on separate Forms 1933. Therefore, we are unable to answer the questions concerning disciplinary actions taken or employee reimbursements received for the individual items, other than to state that no disciplinary actions were evident from the documentation provided. An analysis of these items showed that 17 of the 50 communication and surveillance devices were in excess of 10 years old at the time of the loss; 8 of the 17 were in excess of 15 years old.

The first of the two lost communication devices was misplaced during shipment to the manufacturer for testing purposes. The shipping company subsequently reimbursed the government \$100 for the communication device and \$13.27 for the cost of shipping. Documentation recorded on the Form 1933 indicated that no disciplinary action was recommended for the employee involved. The second communication device was lost during shipment between IRS offices. Documentation provided by the IRS did not indicate whether any disciplinary action was taken. The IRS procured this communication device in May 1995, and it was lost in December 1999.

Based on documentation provided, disciplinary actions associated with the 20 lost and 13 stolen identification badges/commissions included 3 instances where employees were counseled and 2 instances where employees were directed to reimburse the government for the cost of the badge/commission. Disciplinary action was not taken in 9 instances, and we could not determine if disciplinary actions were taken in the remaining 19 instances.

## **Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service**

---

---

### **Missing Computers Containing Confidential Taxpayer Information**

---

We evaluated the possibility that confidential taxpayer information resided on the 75 applicable missing computers.<sup>4</sup>

Through documentation provided by the IRS, we determined that for the two lost computers, the hard drive on one was cleared of all files, and the hard drive on the second was removed prior to the loss. Each loss occurred during the shipping of these two computers. A similar situation existed for the one stolen computer in that its hard drive was also reported to be cleared of all files during the shipment process and before the theft.

As for the 68 computers that were unaccounted for during physical inventory, and the 4 computers for which no documentation could be provided, we were unable to determine if confidential taxpayer information was present on the computers. We determined that at least 19 of the 68 computers were assigned to either the IRS' examination or collection functions, which would have the potential for having taxpayer information contained on the hard drives.

---

### **Sufficiency of File Encryption Practices**

---

The Department of the Treasury issued a memorandum dated February 15, 2001, providing guidance on protecting classified and sensitive information on laptop computers. This document requires encryption for all data on a classified laptop, but does not specifically provide for encryption of sensitive but unclassified information. The IRS is working on a draft laptop security policy that provides for file encryption for all IRS laptop computers storing sensitive but unclassified information, such as taxpayer data.

The above draft policy and requirements pertain to laptop computers as they currently exist at the IRS. Therefore, the following discussion and related tests only pertain to laptop computers currently deployed by the IRS. We were informed that no encryption policy or requirements exist for desktop computers.

---

<sup>4</sup> 100 missing computers in our sample, less the 13 that were disposed of without updating the inventory records, and the 12 that were subsequently located.

## Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

---

The encryption software used by the IRS is designed to encrypt data residing in specific file folders on an internal drive. The specified file folders are established as the computer's default settings and a user who saves files to locations that are not specified by the encryption software will not be encrypted. Once a file is encrypted, a key phrase, which is longer and more involved than a basic password, is needed to open the file in a readable format.

To test the adequate implementation of the encryption requirements, we judgmentally selected 11 laptop computers used by IRS examination employees, and 5 laptop computers used by IRS collection employees located in 2 field posts-of-duty for an unannounced verification of encryption practices.<sup>5</sup>

The results of our very limited test showed that five of the laptops did not have encryption software installed. This was because the encryption software used by the IRS was not compatible with the operating system used on these older-type laptops.<sup>6</sup> We observed taxpayer information on each of these five laptops. Further, even though the remaining 11 laptop computers did have the encryption software installed, we observed unencrypted taxpayer information on 5 of the 11 laptops. This condition occurred because the information was saved to a location on the hard drive that was not protected by the encryption software.

To prevent unauthorized access to programs and files maintained on IRS laptop computers, the IRS makes use of an operating system password access control. By using this method, an employee must have a system-recognized login name and password to gain access to the computer.

Our tests of the 16 judgmentally selected laptop computers showed that all were protected by the operating system password access control.

---

<sup>5</sup> The examination employees' computers use a Windows NT operating system; the collection employees' computers use a Unix operating system.

<sup>6</sup> These older-type laptops used the Unix operating system.

## **Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service**

---

Though this control does provide a deterrent to prevent an unauthorized individual from powering-up the computer and accessing programs and data through the computer's installed operating system, it can be compromised by a knowledgeable and determined individual to gain access to unencrypted files maintained on the computer's hard drive. The ability to gain access in this manner greatly increases the necessity to encrypt all files that contain taxpayer information.

The CIO's Office of Security is responsible for establishing the IRS' policy and requirements concerning the prevention of unauthorized disclosure of taxpayer information maintained on laptop computers and the use of encryption software to ensure this prevention. The individual IRS business units are responsible for the actual implementation of the policy and requirements. However, neither the Office of Security nor the individual business units conduct specific reviews to confirm that the established policy and requirements are actually being followed; i.e., checking field laptops for unencrypted taxpayer information maintained on their hard drives.

Although our limited test is not statistically valid and thus may not be representative of conditions throughout the IRS, we believe that our observations warrant immediate attention by IRS security and operating divisions' management to alert computer users of the need to implement and adhere to security and encryption practices. We are also referring this issue to our Information Systems Program audit staff for consideration of a more thorough review to determine the extent to which the IRS is at risk of unauthorized disclosure of taxpayer information.

---

### **Reports of Survey (Forms 1933) Not Properly Filed**

---

#### **Computers**

We analyzed the completeness of Forms 1933 on the 68 computers that were unaccounted for during a physical inventory, the 2 lost computers, and the 1 stolen computer. Our results showed that the forms were not always prepared, or completely prepared, for the reported missing computers.

In all instances, the back of the Form 1933, which records recommendations for disciplinary actions and includes the

## **Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service**

---

signatures of the responsible management officials recommending those actions, was not filled out, or the IRS was unable to provide the back of the form.

Specifically, for the 68 unaccountable computers, 34 were reported on a Form 1933 without including acquisition dates or cost amounts; 9 were reported on a Form 1933 without the form being signed by the property officer, in addition to not containing all the required information; 22 were reported via memoranda; and, 3 were reported via e-mails. One of the lost computers was reported on a Form 1933 without showing the acquisition date and cost amount. The other lost computer was reported on a Form 1933 without being signed by the property officer or completely filled out. The one stolen computer was reported via an e-mail.

In addition, we are unable to comment on the 4 missing computers for which no documentation was provided.

### **Investigative Items**

We analyzed the completeness of Forms 1933 on the 6 missing firearms, the 50 investigative items that were unaccounted for during physical inventory, and the 22 lost and 13 stolen investigative items. Our results showed that the forms were not always prepared, or completely prepared, for the reported missing firearms and investigative items.

Specifically, for the six firearms, only one Form 1933 was completely prepared. In four instances, the back of the form was either blank or not provided. In the remaining instance, the form was not prepared. In addition, cost data was not recorded on two forms, and the property officer's signature was not evident on one form.

For the 50 investigative items unaccounted for during a physical inventory, 4 were reported on a complete Form 1933; 14 were reported on a Form 1933 without the back page being filled out; 29 were reported on a Form 1933 that did not include a back page; and, 3 were reported via a memorandum. In addition, required cost data was not provided on 7 items, the acquisition date was not shown on 5 items, and the property officer's signature was not shown on the front of the Form 1933 on 5 items.



## Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

---

For the 22 lost investigative items, 6 were reported on a complete Form 1933; 5 were reported on a Form 1933 without the back page being filled out; and, 11 were reported on a Form 1933 that did not include a back page. In addition, required cost data was not provided on one item, and the property officer's signature was not shown on the front of the Form 1933 on two items.

For the 13 stolen investigative items, 4 were reported on a complete Form 1933; 2 were reported on a Form 1933 without the back page being filled out; and, 7 were reported on a Form 1933 that did not include a back page. In addition, required cost data and acquisition dates were not provided on two items.

The IRS' *Personal Property Management Handbook*, dated July 1998, requires in cases of lost or damaged property that all available information, including accurate identification of the property to be surveyed and all prior actions taken, be recorded on Form 1933. Further, it requires that the investigating official establish the amount of the loss, cause of the loss, who is responsible for the loss, and any previous instances of negligence by the person involved. The findings established and any recommendations are to be reported on the Form 1933 and forwarded to an approving official. The approving official is responsible for either concurring with or disapproving the recommendations. In either case, the approving official is required to sign page two of the Form 1933.

Without completely preparing the Forms 1933, including evidence of responsible official signatures, the IRS cannot assure that items of inventory are accurately accounted for, and that accountability is established for items that are lost or stolen.

### Recommendations

In addition to previous recommendations made by GAO and us to improve property management, the IRS should take the following steps to improve the reporting of missing property and to ensure that adequate security and encryption practices are followed.

## **Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service**

---

1. The CIO and the Chiefs, CI and Agency-Wide Shared Services, should collaborate to re-emphasize existing procedures to ensure that Forms 1933 are completely prepared when warranted and that all responsible officials properly sign the forms to evidence their review.

Management's Response: The CIO and the Chiefs, CI and Agency-Wide Shared Services, will jointly issue an alert to all IRS organizations re-emphasizing the requirement to properly complete, sign, and date the Form 1933, when warranted.

Office of Audit Comment: In providing additional information on disciplinary action, the IRS response provided that it is the responsibility of the investigation organization (TIGTA) to make recommendations concerning disciplinary actions subsequent to proper investigation. We would like to clarify that TIGTA's Office of Investigations, through its Report of Investigation, does not recommend disciplinary action when advising the IRS of the results of its investigation on these matters. IRS management is responsible for deciding on the proper course of and administering disciplinary action.

2. The CIO should immediately issue an alert to all IRS employees advising of applicable security and encryption practices, and instructing managers to confirm that these practices are in place and functioning as intended.

Management's Response: Actions are currently underway to encrypt sensitive but unclassified information on all laptop computers, without negatively affecting ongoing work being performed on older laptop computers. New laptop computers are being configured with software to encrypt taxpayer information. IRS employees have been instructed on the need to encrypt files containing taxpayer information. Action will be taken to reiterate this requirement where the encryption capability has not been used.

### **Detailed Objectives, Scope, and Methodology**

The overall objective of this limited scope review was to assess the sufficiency of Internal Revenue Service (IRS) systems and procedures in providing select management information concerning missing computers and other sensitive items of inventory, such as value of the loss, associated employee disciplinary actions, and possible disclosure of taxpayer data. We also assessed the sufficiency of controls used to protect taxpayer information that is stored on laptop and desktop computers. The scope of our review involved a sample of missing computers, and all identified other sensitive items of inventory as reported by the IRS and included in our previous report.<sup>1</sup> In doing so, we attempted to collect sufficient information to respond to the Senate Finance Committee's questions. To accomplish our objective, we:

- I. Reviewed Reports of Survey (Forms 1933), and other documentation for a judgmental sample of 100 randomly selected items from the list of reported 2,332 missing computers provided by the IRS, and all missing firearms and sensitive investigative equipment, to identify:
  - A. The approximate value of the missing item at the time of the loss.<sup>2</sup>
  - B. Whether the missing items were lost, stolen, or destroyed.
  - C. The types of disciplinary actions taken against employees found to be responsible for a loss or theft.
  - D. What follow-up there has been on lost or stolen computers.
  - E. To what extent IRS employees have reimbursed the government for missing computers.
  - F. How many of the missing computers were the responsibility of a senior manager, and what disciplinary action was taken.
  - G. If any individual has missing more than one computer, and what disciplinary action was taken against that individual.
  - H. How many missing computers contained confidential taxpayer information.

---

<sup>1</sup> *Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service* (Reference Number: 2002-10-030, dated November 2001).

<sup>2</sup> In the report, where available we provided the acquisition costs and the depreciated value at the time of the loss, using straight-line depreciation, no residual value, and a useful life corresponding to the type of property. We did not calculate replacement costs, as the detailed information needed to make decisions on like-kind replacements was not always available, and significant, rapid advances in technology would make comparisons difficult.

## **Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service**

---

- I. How many missing items did not have a Form 1933 prepared or not fully prepared.
- J. The responsible managers who failed to properly file a Form 1933 for a missing computer.

**SAMPLE BASIS:** From the file of 2,332 missing computers provided by the IRS, we first segregated the file into 2 sub-files; 1 containing 4 offices that comprised 87 percent of all missing computers, and 1 file containing the balance of the missing computers. We randomly selected 50 items from each sub-file for a total sample of 100 items. We used a judgmental sample, as we did not intend to project the sample results.

- II. Assessed the sufficiency of the IRS' encryption practices of taxpayer data maintained on desktop and laptop computers to prevent the unauthorized disclosure of such data if the computer was lost or stolen.
  - A. Discussed encryption practices with appropriate IRS personnel.
  - B. Identified the IRS' policies concerning taxpayer data maintained on desktop or laptop computers, and to what extent this data must be encrypted.
  - C. Identified the type of information source that would be most susceptible to the disclosure of taxpayer data.
  - D. Judgmentally selected a sample of employees' computers and verified:
    - 1. Logon protection to access the computer itself.
    - 2. Logon protection to access any downloaded files (assuming encryption of data).
    - 3. Downloads of taxpayer data were encrypted.
    - 4. That no related taxpayer data was maintained on the hard drive that was not encrypted (i.e., memos to file, taxpayer correspondence, notes of examinations or collection efforts, etc.).

**SAMPLE BASIS:**

We judgmentally selected 11 laptop computers used by IRS examination employees, and 5 laptop computers used by IRS collection employees, located in a San Francisco Small Business/Self Employed Division office, and an Atlanta Tax Exempt and Government Entities Division office. The sample included one Compaq, four Micron, six Dell, and five IBM laptop computers. We used a judgmental sample, as we did not intend to project the sample results. We worked with the employees to access their computers through the operating system, first by attempting to logon ourselves, and then having the employees logon if we could not. Employees also assisted in accessing and identifying the files maintained on their hard drives.

- E. Assessed whether files contained on a hard drive could be accessed if the hard drive was installed on another computer.

**Major Contributors to This Report**

Daniel R. Devlin, Assistant Inspector General for Audit (Headquarters Operations and Exempt Organizations Programs)

John R. Wright, Director

Thomas J. Brunetto, Audit Manager

Theodore Grolimund, Senior Auditor

Terrey Haley, Senior Auditor

S. Kent Johnson, Senior Auditor

Larry Reimer, Senior Auditor

Bobbie M. Draudt, Auditor

Midori Ohno, Auditor

Peter L. Stoughton, Auditor

**Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of  
Inventory at the Internal Revenue Service**

---

**Appendix III**

**Report Distribution List**

Deputy Commissioner N:DC  
Commissioner, Small Business/Self-Employed Division S  
Commissioner, Tax Exempt and Government Entities Division T  
Deputy Commissioner for Modernization and Chief Information Officer M  
Chief, Agency-Wide Shared Services A  
Chief, Criminal Investigation CI  
Chief Financial Officer N:CFO  
Director, Enterprise Systems and Asset Management M:I:E:CP:T:A  
Director, Office of Security M:S  
Director, Security Evaluation and Oversight M:S:S  
Chief Counsel CC  
National Taxpayer Advocate TA  
Director, Legislative Affairs CL:LA  
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O  
Office of Management Controls N:CFO:F:M  
Audit Liaisons: Commissioner, Small Business/Self-Employed Division S  
Commissioner, Tax Exempt and Government Entities Division T  
Deputy Commissioner for Modernization and Chief Information Officer M  
Chief, Agency-Wide Shared Services A  
Chief, Criminal Investigation CI  
Chief Financial Officer N:CFO

**Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service**

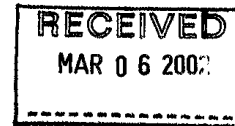
**Appendix IV**

**Management's Response to the Draft Report**



DEPUTY COMMISSIONER


DEPARTMENT OF THE TREASURY  
INTERNAL REVENUE SERVICE  
WASHINGTON, D.C. 20224



**MAR 6 2002**

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR TAX  
ADMINISTRATION

FROM:

*for*   
John D. Weede  
Deputy Commissioner for Modernization &  
Chief Information Officer

SUBJECT:

Draft Management Advisory Report - Follow-on Review of  
Lost or Stolen Sensitive Items of Inventory at the Internal  
Revenue Service (Audit #200210015)

This memorandum serves as the management response to the follow-on review to our initial November 2001 response to the *Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service (IRS)*, (Reference No.: 2002-10-030). The Modernization, Information Technology & Security Services (MITS) organization responded to both inquiries, with input provided from the Chief, Criminal Investigation (CI) contained within the initial November 2001 response.

Recognizing the importance of asset management, we have taken significant steps recently to improve our ability to manage the information technology (IT) inventory. As a result, the IRS has shown consistent improvement in General Accounting Office audits of our inventory control since 1999. We consolidated the responsibility for inventory control under MITS and dedicated staff to maintain the inventory. This centralized controlling authority has created a uniform set of rules and procedures for the acquisition, management and disposal of agency computers. In 2001, we upgraded our inventory tracking system to facilitate the tracking and verification of 163,000 computers at over 700 sites. As we acquire and deploy new computers, we are committed to improving our ability to manage and control the Service's IT assets.

The Honorable Charles E. Grassley requested the Treasury Inspector General for Tax Administration (TIGTA) conduct a follow-on assessment of IRS's reporting of missing computers and other sensitive items. The IRS provided the requested information to TIGTA on the valuation of the missing items, status of disciplinary action, and the Forms 1933 for the sample of 100 records.

## Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

---

In our review of the draft report, we would like to provide the following information:

### **Value of missing computers and identification of lost, stolen or destroyed status**

- We concur with the classification, analysis, and the valuation of the representative sample of 100 computers.
- Of the 68 computers unaccounted for, the IRS is working to locate these systems using our Enterprise System Management tool Tivoli.
- Of the 12 computers subsequently located by the IRS, documentation has been provided to TIGTA for verification.
- We have strengthened our tracking system by implementing a new Asset Management Inventory Tracking System (ITAMS) in March 2001.
- During July 2001, we implemented a formalized Annual Certification Process, which closely accounts for individual computer equipment.
- We have improved the IRM for Asset Management. An interim version will be issued shortly.
- We implemented an updated Disposal Process that coordinates both the Agency-Wide Shared Services (AWSS) and MITS organization activities.
- In July 2001, we established standard naming conventions to improve inventory management. For example, "PC" will be used consistently throughout the inventory management process.
- We have implemented a systems management tool (Tivoli) to allow MITS to discover devices on the IRS network, which is an additional means to verify the hardware in the inventory.

### **Disciplinary actions taken and government reimbursement**

- The first of the two lost computers was lost during shipment from the manufacturer after repairs and was subsequently replaced by the manufacturer.
- The second of the two lost computers was being excessed to the Volunteer Income Tax Assistance (VITA) program, because it was over 3 years old. During shipment to VITA, the system was misplaced. A Report of Survey, Form 1933, was completed and forwarded to TIGTA indicating that the system was not received by VITA. It is the responsibility of the investigation organization (TIGTA) to make recommendations concerning disciplinary actions subsequent to proper investigation. No documentation was found that indicates any disciplinary actions were recommended or taken.
- The one stolen computer was reported to TIGTA for their investigation. To date, we have not received any recommendations for disciplinary action.

### **Missing computers containing confidential taxpayer information**

- The IRS policy is to degauss and/or purge system hard drives prior to excessing equipment and the completion of Report of Excess Personal Property, GSA Standard Form 120.



## Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

---

- Of the 68 computers, 19 were assigned to IRS examination or collection functions, which could have the potential for having taxpayer information contained on their hard drives. However, through the years, business units adopted different security mechanisms such as the use of file encryption and/or the policy prohibiting the storage of sensitive but unclassified information on the hard drives to protect taxpayer information.

### **Sufficiency of File Encryption Practices**

- Decisions on required security mechanisms at the IRS have historically been based on Federal policies and a risk management approach. Under this approach, technology risks and disclosure vulnerabilities were balanced against cost, operational overhead, and business impact. Older laptops computers used by various operating units were independently acquired using this approach. They each use a different combination of physical, technical, and management control strategies to protect sensitive information.
- Although no formal policy exists that requires the encryption of sensitive but unclassified information on all IRS laptop computers, actions are underway to establish such a policy, without negatively affecting ongoing work being performed on older laptop computers. New laptop computers being acquired to process taxpayer information are being configured with software to encrypt taxpayer information and IRS employees using these laptops will be instructed on the need to encrypt taxpayer files.
- For example, the five UNIX laptop computers, referenced in your report, assigned to the IRS collection employees are being replaced with new computers running a new Integration Collection System (ICS/NT) that is based on the Windows NT operating system. These new laptops will have encryption software installed.

### **Reports of Survey (Forms 1933) not properly filed**

We concur with the assessment made by TIGTA on the completeness of Report of Survey, Form 1933. New IRM procedures being implemented will stipulate that required information and appropriate IRS management signatures be included on the form. Based on TIGTA recommendations, IRS management will take appropriate action.

## Management Advisory Report: Follow-on Review of Lost or Stolen Sensitive Items of Inventory at the Internal Revenue Service

---

We concur with your two recommendations and can assure you that the following actions will be completed as soon as possible.

### **Recommendation #1:**

The CIO and the Chiefs, CI and Agency-Wide Shared Services, should collaborate to re-emphasize existing procedures to ensure that all Report of Survey, Form 1933 are completely prepared when warranted and that all responsible officials properly sign the forms to evidence their review.

### **Response:**

Concur - The CIO, and the Chiefs of CI and Agency-Wide Shared Services (AWSS) will jointly issue an alert to all IRS organizations re-emphasizing the requirement to properly complete, sign and date the Report of Survey, Form 1933, when warranted. These procedures and processes are outlined in IRMs and procedural documents currently in force. We agree to re-emphasize these existing documents and reinforce the need to comply.

### **Recommendation #2:**

The CIO should immediately issue an alert to all IRS employees advising of applicable security and encryption practices, and instructing managers to confirm that these practices are in place and functioning as intended.

### **Response:**

The IRS has been actively pursuing an upgrade of its laptop computers to improve tax processing capabilities. The upgrade includes the use of encryption software on laptop computers used to process taxpayer information. In addition, actions are currently underway to encrypt sensitive but unclassified information on all laptop computers, without negatively affecting ongoing work being performed on older laptop computers. New laptop computers being acquired to process taxpayer information are being configured with software to encrypt taxpayer information. IRS employees using these laptops have been instructed on the need to encrypt files containing taxpayer information. Encryption tools will be implemented to the fullest extent practical. Based on the TIGTA finding that the encryption capability was not always being used, action will be taken to reiterate this requirement.

MITS looks forward to working with TIGTA to address all issues and recommendations and to help facilitate the successful closing of this audit. If you or members of your staff have any questions, please contact me at (202) 622-6800 or you may also contact Thomas Mulcahy, Office Manager, Program Oversight and Coordination, at (202) 283-6063.

cc: Chief, Criminal Investigation  
Commissioner, Small Business and Self Employed Division